1. Introduction to Cyber Security

✅ 1. What is Cybersecurity?

Cybersecurity is the practice of **defending systems, networks, applications, and data** from digital attacks, unauthorized access, damage, or theft.

It combines **technology**, **processes**, and **people** to protect the **Confidentiality, Integrity, and Availability (CIA)** of digital assets.

🎯 2. What are the Core Principles of Cybersecurity (CIA Triad)?

Principle	Meaning
Confidentiality	Protecting sensitive data from unauthorized access (e.g., encryption, access controls).
Integrity	Ensuring data is trustworthy and unaltered (e.g., hashing, checksums, file monitoring).
Availability	Ensuring systems and data are accessible to authorized users when needed (e.g., redundancy, uptime).

🔐 3. How Does Encryption Contribute to Security?

Encryption transforms readable data (**plaintext**) into unreadable data (**ciphertext**) using an algorithm and a key.

🔑 **Key Concepts:**

- **Symmetric encryption** (e.g., AES): same key for encryption/decryption.
- **Asymmetric encryption** (e.g., RSA): public/private key pair.
- **At rest**: Full disk encryption, encrypted databases.
- **In transit**: TLS/SSL for web traffic, SSH for remote login.

🔒 **Purpose**:

- Maintains **confidentiality**.
- Helps with **integrity** when paired with hashing.
- Prevents data breaches from exposing sensitive information.

📊 4. What is Risk Management in Cybersecurity?

Risk management is the process of:

1. **Identifying** potential threats/vulnerabilities.
2. **Assessing** the likelihood and impact of those risks.
3. **Mitigating** through controls or strategies.
4. **Monitoring** and reviewing risks continuously.

🧠 **Key Terms:**

- **Asset**: What you're protecting (e.g., data, systems).
- **Threat**: Potential danger (e.g., hacker, malware).
- **Vulnerability**: Weakness that could be exploited.
- **Risk**: Likelihood × Impact of a threat exploiting a vulnerability.

Frameworks like **NIST RMF** and **ISO 27005** guide formal risk management processes.

☠️ 5. What are the Different Types of Cybersecurity Threats?

Threat Type	Description
Malware	Malicious software (viruses, worms, Trojans, ransomware).
Phishing	Deceptive emails or websites used to steal credentials/data.
Ransomware	Encrypts data and demands ransom.
DDoS	Flooding services to make them unavailable.
Zero-Day Exploit	Exploiting unknown or unpatched vulnerabilities.
Insider Threats	Internal users intentionally or unintentionally causing harm.
MitM Attacks	Intercepting communication between two parties.
SQL Injection	Injecting malicious SQL queries into input fields.
Cross-Site Scripting (XSS)	Injecting scripts into web pages to hijack sessions or deface sites.

🧬 6. What is the Difference Between a Virus and a Worm?

Aspect	Virus	Worm
Spread	Needs user interaction to spread (e.g., run file).	Self-replicates and spreads autonomously via network.
Infection	Attaches to legitimate files or programs.	Exploits system/network vulnerabilities directly.
Example	Macro viruses in documents.	WannaCry (2017) exploited SMB protocol.

🎭 7. What is Social Engineering in the Context of Security?

Social engineering is the manipulation of people into performing actions or revealing confidential information.

🛠️ **Common Techniques:**

- **Phishing** – Fake emails or websites.
- **Vishing** – Phone-based social engineering.
- **Smishing** – SMS-based phishing.
- **Pretexting** – Creating a fabricated scenario (e.g., posing as IT).
- **Tailgating** – Gaining physical access by following someone into a secure area.

🧠 *Humans are the weakest link — social engineering exploits trust, urgency, or fear.*

🧱 8. What are the Key Components of an Information Security Program?

1. **Governance** – Policies, risk management, compliance.
2. **Asset Management** – Knowing and classifying assets.
3. **Access Control** – Identity management, least privilege.
4. **Threat Management** – Vulnerability scanning, patching, red teaming.
5. **Incident Response** – Detection, containment, eradication, recovery.
6. **Security Awareness Training** – Educating users.
7. **Monitoring & Auditing** – SIEMs, logs, threat hunting.
8. **Business Continuity/DR** – Backup, failover, disaster recovery plans.

🧭 9. How Do Security Policies and Frameworks Contribute to an Organization's Security Posture?

- **Security policies** are formal documents that define how an organization protects its assets.
- **Frameworks** provide structured approaches for implementing security (e.g., NIST, ISO 27001, CIS).

Benefits:

- Aligns security with business objectives.
- Ensures regulatory compliance.
- Sets expectations for behavior and responsibilities.
- Establishes repeatable processes (e.g., access reviews, patch cycles).
- Provides metrics for audits and improvements.

🌐 10. What is the Purpose of the OWASP Top Ten?

The **OWASP Top Ten** is a widely recognized list of the **top 10 most critical web application security risks**.

Purpose:

- **Educate** developers, security teams, and architects.
- **Standardize** web app security awareness.
- **Prioritize** mitigation of high-impact, common vulnerabilities.

Example Risks:

- A01: Broken Access Control
- A03: Injection (e.g., SQL, LDAP)
- A07: Identification & Authentication Failures
- A08: Software & Data Integrity Failures

🧠 Knowing OWASP Top Ten is **essential** for web pentesters and defenders alike.

🧍 11. What is the Role of Access Control in Cybersecurity?

Access control is about ensuring **only authorized users** can access **specific resources**, and only to the **extent required**.

Types:

- **DAC (Discretionary Access Control)** – User-defined (e.g., file ownership).
- **MAC (Mandatory Access Control)** – System-enforced rules (e.g., military classification).
- **RBAC (Role-Based Access Control)** – Access based on roles.
- **ABAC (Attribute-Based Access Control)** – Access based on policies and attributes.

🔐 Enforces **least privilege** and **separation of duties**.

🔑 12. How Does Multi-Factor Authentication (MFA) Enhance Security?

MFA requires **two or more** of the following:

1. **Something you know** – password or PIN.
2. **Something you have** – phone, hardware token.
3. **Something you are** – biometrics (fingerprint, face ID).

📍 Adds an **extra layer** beyond passwords — even if credentials are compromised, unauthorized access is unlikely without the second factor.

🌐 13. What Are the Common Methods for Securing a Network?

1. **Firewalls** – Control inbound/outbound traffic (stateful/stateless).
2. **IDS/IPS** – Detect or block malicious traffic (Snort, Suricata).
3. **Segmentation/VLANs** – Isolate traffic for security and performance.

4. **VPNs** – Encrypt remote connections.
5. **Zero Trust Model** – Never trust, always verify (microsegmentation, strict access).
6. **Network Access Control (NAC)** – Evaluate endpoint posture before allowing connection.
7. **Regular Patching** – Secure routers, switches, firewalls.
8. **Wireshark / Packet Analysis** – Monitor traffic and detect anomalies.
